SecurityGen

Telecom Security. Transcending Generations.

5G Standalone Security

2024 update - new attack techniques

Version Number: **1.0**

Date: **Sep 2024**

Author(s): **Igor Pigalitsyn, Dmitry Kurbatov**

Table of Contents

2 **Introduction**

- Objectives of the white paper
- A bit about key components of 5G Core network
- Common security challenges and threats in 5G
- Existing handy 5G security material

6 **New attack technique - Network Manipulation via NF Instance Profile Update**

- Context of the new vulnerability
- How it was discovered
- Comparison with other known vulnerabilities
- Technical explanation of the vulnerability
- Potential impact and exploitation scenarios
- Likelihood of Occurrence
- Tactics, Techniques, and Procedures (TTPs)
- Steps to protect against such exploitation

16 **Conclusion**

17 **Additional materials**

- References

01. Introduction

1.1. Objectives of the white paper

5G mobile networks are gradually being rolled out by operators worldwide. Given that deploying a network capable of delivering all the new expected functionalities is a complex and expensive process, the 3GPP specifications describe two possible tracks for 5G development:

- **Non-Standalone (NSA):** An interim implementation that relies on existing LTE radio and 4G core components as the base for selectively adding 5G components on top.

- **Standalone (SA):** A network implementation mode that uses only new components, such as 5G New Radio (5G NR) and 5G Core Network (5GC).

This research focuses on the SA mode of 5G network deployment. The implementation is based on 3GPP Release 15, with the OpenAPI Specification providing detailed descriptions of each interface.

1.2. A bit about key components of 5G Core network

The 5G SA core network comprises several essential components that serve subscribers (Figure 1), but not only:

- **Access and Mobility Management Function (AMF):** Manages subscriber registration, connections, and location.

- **Session Management Function (SMF):** Handles sessions, manages tunnels between the access network and User Plane Function (UPF), selects the UPF gateway, and allocates IP addresses.

- **User Plane Function (UPF):** Connects subscribers to the Internet, handles GTP-U packets, assigns policy rules, and sets quality of service parameters.

- **Network Repository Function (NRF):** Maintains a repository of profiles for network functions. Each function must register its status, capabilities, and options.

- **User Data Management (UDM):** Manages user profiles, IDs, and generates authentication credentials.

- **Unified Data Repository (UDR):** Stores and extracts subscriber-related data.

- **Authentication Server Function (AUSF):** Acts as the authentication server for both 3GPP and non-3GPP access.

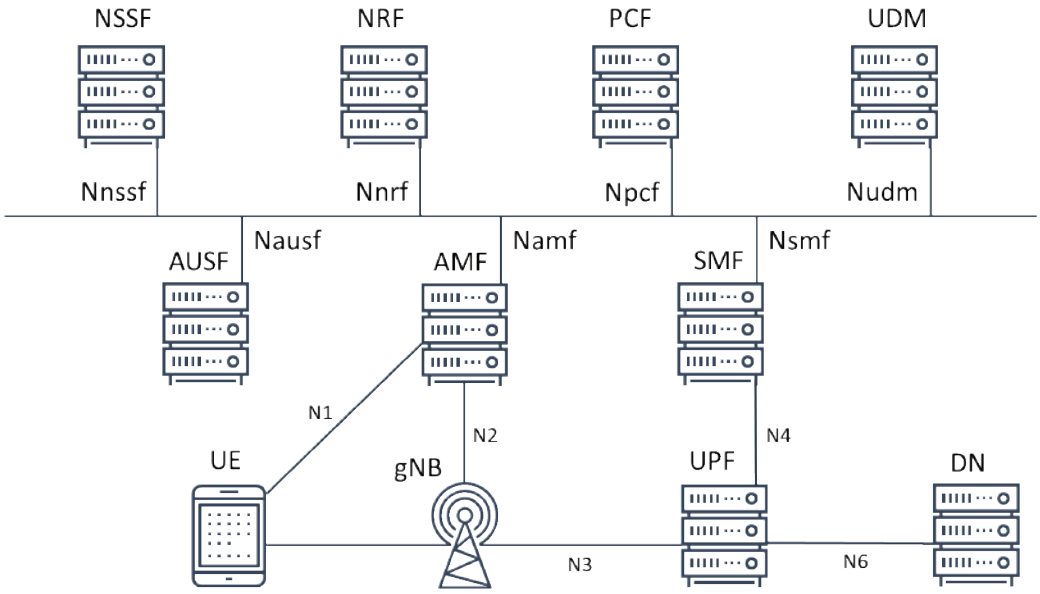

Figure 1

The 5G architecture supports two types of interaction between network functions: interface-based and service-based.

- **Interface-Based Interaction:** Describes point-to-point interactions between network function services (e.g., the N11 interface), which is a familiar approach from previous network generations.

- **Service-Based Architecture (SBA):** A new approach where network elements are connected by a single bus, allowing authorized control plane (CP) network functions to access the services of other NFs.

This architecture uses the HTTP/2 protocol and REST API for interaction between services, making the system more flexible and easier to describe. Additionally, 5G networks use the GTP-U and PFCP protocols.

In this paper, we will explain the security challenges associated with this technological stack, as it presents possibilities for attacks on subscribers and the operator's network. Such attacks can originate from international roaming networks, the operator's network, partner networks providing access to services, and other adjacent network segments.

1.3. Common security challenges and threats in 5G

Although in this paper we will focus on the security of the Core Network, it is important to mention that the deployment of 5G networks brings with it a host of new security challenges and threats, some of which are unique to mobile technology and some are relevant across all ICTs. Just to name a few:

- **Cellular Technology and OpenRAN:** The cellular aspect of 5G introduces new challenges, particularly with the inclusion of OpenRAN. OpenRAN aims to promote flexibility by allowing different vendors to provide various components of the radio access network. However, this openness also increases the attack surface, making it vital to ensure the security of each component and the interfaces between them.

- **Virtualization and Containers:** The technologies used to deploy network functions in the cloud introduce new security risks. Virtualized environments can be susceptible to hypervisor attacks, container escapes, and other vulnerabilities that could compromise the entire network infrastructure.

- **Supply Chain Security:** 5G networks rely on complex solutions that involve a long supply chain, which is challenging to secure in a global environment. Ensuring the security of hardware and software components from various suppliers is critical, as any compromised element can become an entry point for attackers.

- **Increased API and Interface Exposure:** To enable better flexibility and new use cases, 5G networks expose a large number of APIs and interfaces. While this enhances network functionality, it also expands the threat landscape. Attackers can exploit vulnerabilities in these interfaces to gain unauthorized access or disrupt network operations.

- **Artificial Intelligence (AI):** AI is increasingly utilized to automate network operations and improve efficiency. However, adversaries can also leverage AI for malicious purposes, such as automating attacks, evading detection, or analyzing network vulnerabilities to plan more effective attacks.

The threat landscape for 5G is constantly evolving, with new threats emerging as the technology matures. Comprehensive threat reports, such as those from ENISA (1) and GSMA (2), detail various potential threats, including advanced persistent threats (APTs), nation-state actors, and sophisticated cybercriminals targeting 5G networks.

1.4. Existing handy 5G security materials

Although there are continuous efforts among different organizations across the globe to enhance the cybersecurity and resilience of 5G networks, here we would like to highlight a few notable initiatives that emerged in 2022 and 2023. In our opinion, these initiatives significantly contribute to the overall objective of implementing better security in 5G infrastructures. These are:

- **ENISA's 5G Security Controls Matrix:** This matrix provides guidance for both standalone and non-standalone 5G networks. It is important to note that the matrix spreadsheet and supporting documentation are available to anyone without charge and without the need to be part of an organization. This accessibility makes it a valuable resource for enhancing 5G security (3).

- **MITRE's FiGHT™ (5G Hierarchy of Threats):** This is a knowledge base of adversary tactics and techniques specifically designed for 5G systems. Modeled after the MITRE ATT&CK® framework, FiGHT's tactics and techniques are complementary to those in ATT&CK, making it an excellent starting point for cybersecurity professionals looking to secure 5G networks (4).

02. New attack technique - Network Manipulation via NF Instance Profile Update

2.1. Context of the new vulnerability

In the 5G core, all network functions communicate with each other via the Service-Based Architecture (SBA). Network functions use HTTP/2 protocol and dedicated interfaces to exchange data. One of the crucial components is the Network Repository Function (NRF), which acts as a central repository for network functions and their capabilities.

In 2023, within our 5G laboratory, we discovered a method to manipulate network configuration by rewriting records stored in the NRF, specifically the instance profiles. This manipulation, if successful and depending on the specific steps taken by the attacker, can result in various consequences, such as Denial of Service (DoS) and Man-in-the-Middle (MiTM) attacks.

2.2. How it was discovered

Initially discovered in mid-2023 in our 5G laboratory, which was established specifically for testing purposes, this attack technique underwent extensive study to develop a solid proof of concept. Once functional exploits were created and tested, the SecurityGen consulting team recommended to some of our customers, who were planning 5G telecom security audits, to include this new technique in their assessment scopes. This recommendation aimed to verify the applicability of the proof of concept across real networks featuring different sets of network functions and vendors.

Subsequently, after conducting four security audits on production 5G networks, and with necessary tuning and adaptation, the proof of concept exploit was validated. The consulting team successfully executed a series of test attacks using this technique, demonstrating its effectiveness.

2.3. Comparison with other known vulnerabilities

An attacker who manages to infiltrate the network segment where such communication occurs can study the communication patterns and use them to masquerade as a legitimate partner, thereby communicating with other network functions.

This scenario is, to some extent, a consequence of two factors present in standalone 5G:

1. **Flexibility in the 5G SBA Architecture:** The idea was that by connecting a new NF to the SBA, it connects to the NRF, uploads information about itself, and after that, it can be used by any other NF.

2. **Absence of Proper Security Measures:** The lack of proper encryption, authentication, and authorization measures has proven to be a common issue, as demonstrated during a series of audits in real-life production networks.

As a result, when applying the Common Vulnerability Scoring System (CVSS) methodology to estimate the severity of this vulnerability, the CVSS 3.0 calculator suggests a score of 8.2. The relevant CVSS vector is:
CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:H.

2.4. Technical explanation of the vulnerability

To manipulate the network configuration, an attacker can send a request to the NRF, which updates the NF instance profile of the network function identified in the request path.

However, before this can be done, the attacker needs to identify the network functions registered in the NRF. To achieve this, the attacker can send a request that returns the nfInstanceID of all network functions currently registered in the NRF.

The attacker executes the /nnrf-nfm/v1/nf-instances GET request. The NRF responds with "200 OK." This response contains the LinksValueSchema, which includes the results of the search for NF instances related to the tested NFs (see Figure 2).

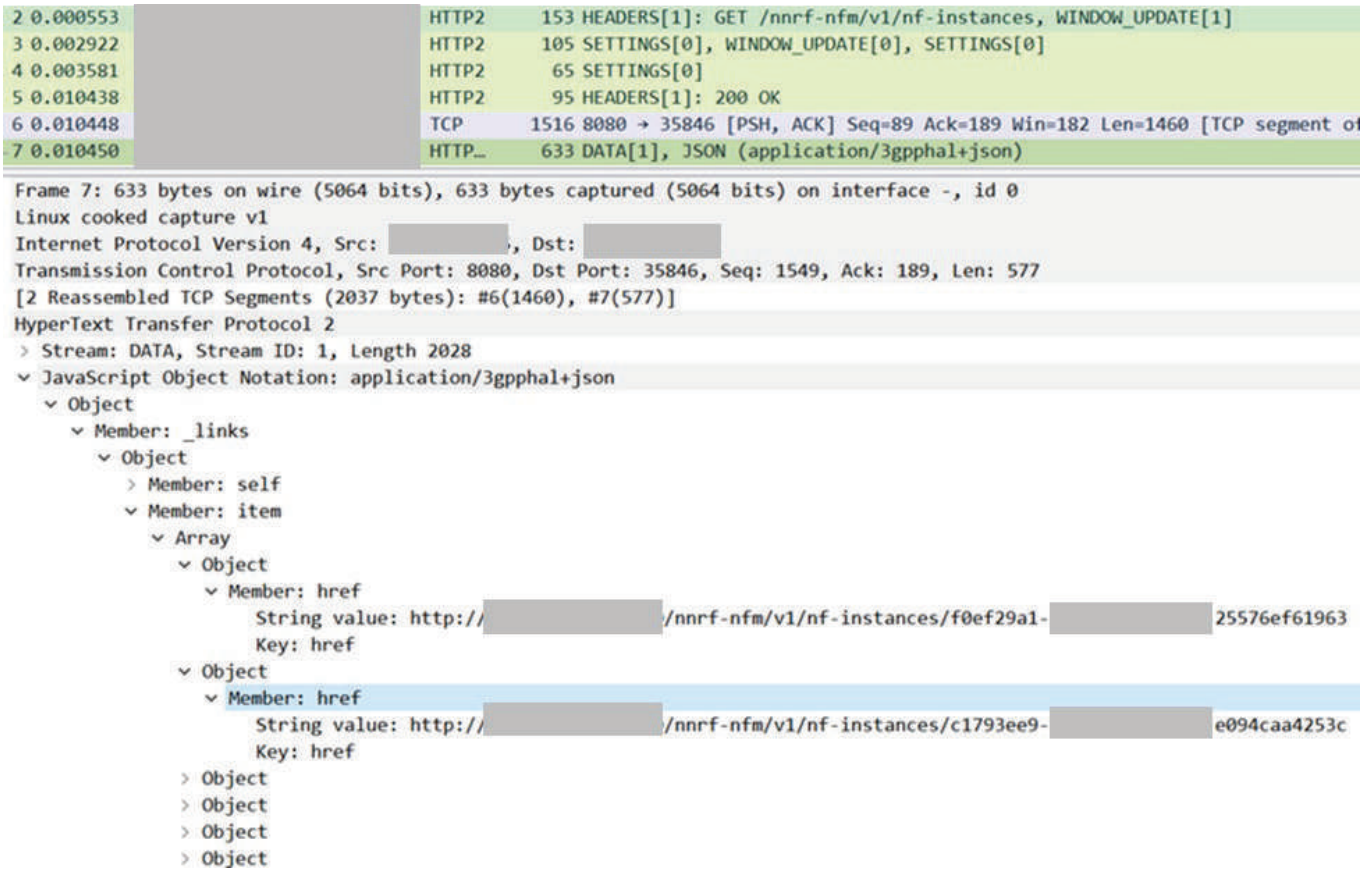

Figure 2

Using this information, attackers can determine the list of URIs of NF instances and leverage the obtained information in subsequent attacks.

After the attacker has identified the list of all network functions registered in the NRF, they can easily extract their NF Profiles. To do this, the attacker can send requests that return the profile of the network function specified by the identifier in the request path.

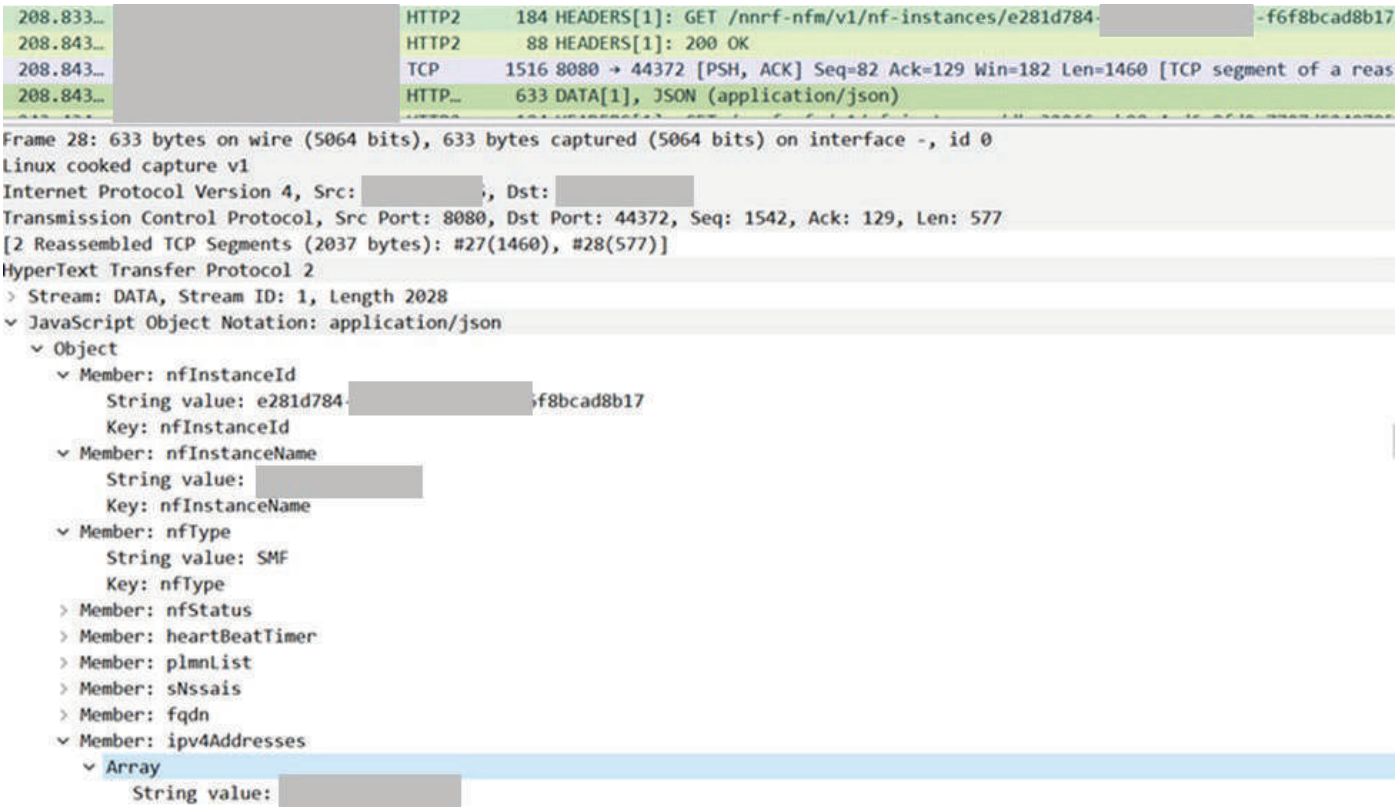

Figure 3

The intruder executed the /nnrf-nfm/v1/nf-instances/{nfInstanceID} GET request. The NRF responded with "200 OK" and the content of the NFProfile component, in which the data of the NF profile was disclosed. This information reveals the entire topology and structure of the network and is crucial for the development of subsequent attacks (see Figure 3).

Now, the attacker is ready to manipulate the network configuration by sending a request to the NRF to update the NF instance profile of the network function identified in the request path.

The attacker executes the /nnrf-nfm/v1/nf-instances/{nfInstanceID} PUT request, substituting fields in the request body, such as the IP address. The NRF responds with "200 OK," confirming the update and including the content of the NF profile component with the updated fields (see Figure 4).

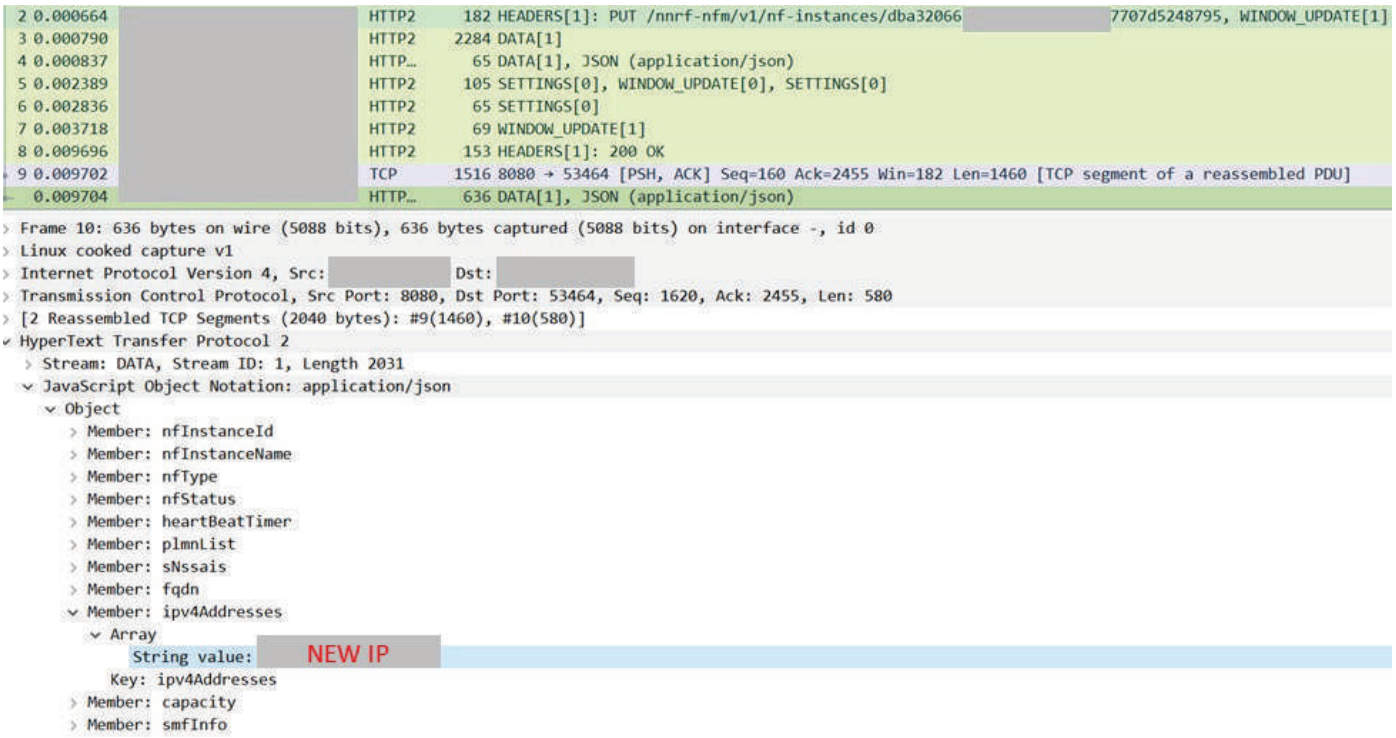

Figure 4

In the case of a Denial of Service (DoS) attack, the attacker can use this request to update the NF instance profile, resulting in the unavailability of the updated NF for 1-2 minutes for newly connected subscribers. This period relates to how quickly the real network function updates its own profile in the NRF – it can be faster, but it is more likely to be longer in production networks. In any case, the attacker can continuously update the profile 1-2 times per minute. Thus, the attack duration does not directly depend on how quickly the NF profile update procedure occurs.

By exploiting this vulnerability, attackers can disrupt network operations and compromise the security and availability of critical network functions.

Alternatively, an attacker can change the IP address in the NFProfile of the victim NF to their own IP. Once other NFs perform the NF Discovery procedure, this will force other network elements to route traffic toward the rogue node. If this logic is implemented successfully, the attacker will effectively achieve a Man-in-the-Middle (MiTM) position, receiving, processing, and forwarding all the traffic passing through their node (see Figure 5).

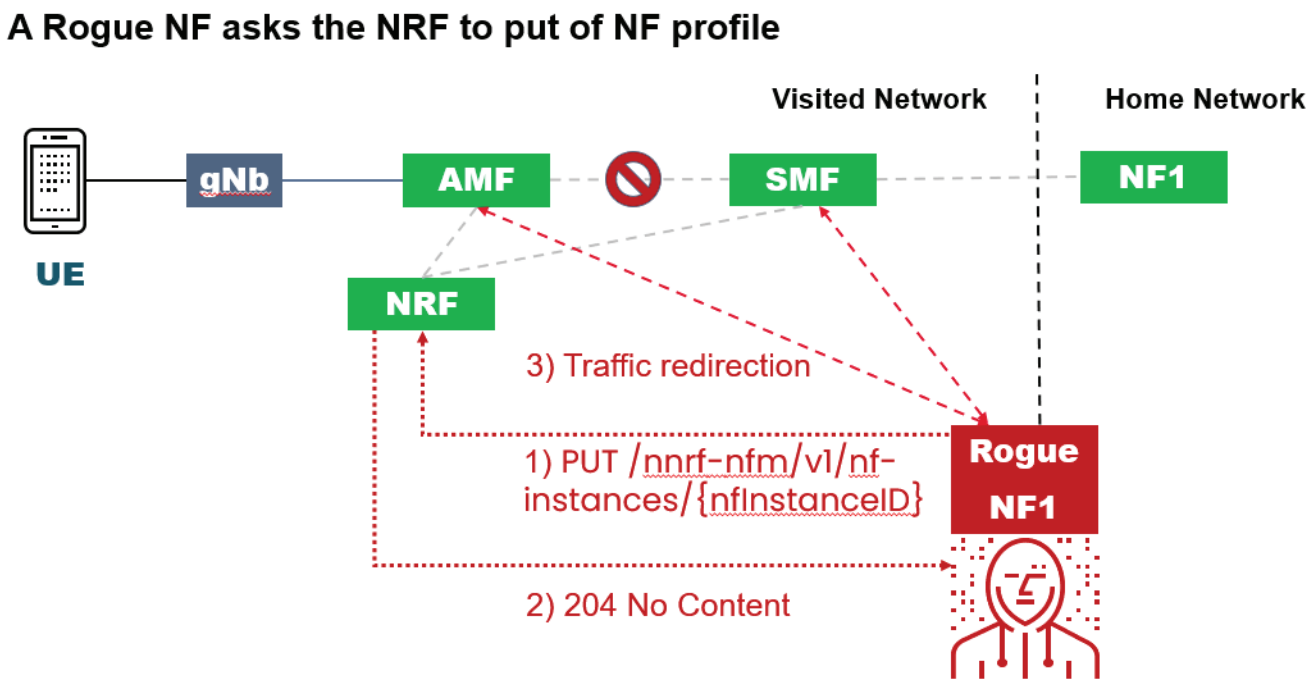

Figure 5

In this position, the attacker can:

- **Read the Information:** Intercept and read the information contained within the traffic, compromising confidentiality.
- **Alter the Data:** Modify the data, thereby affecting its integrity.
- **Drop Packets:** Discard packets, affecting availability and potentially causing disruptions to network services.

By registering a rogue network function, the attacker can severely compromise the security, integrity, and availability of the network, posing a significant threat to overall network operations.

To some extent, this attack can be compared to ARP (Address Resolution Protocol) poisoning in Ethernet networks, which is used to intercept or modify traffic by associating the attacker's MAC address with the IP address of a legitimate network device. Similarly, in the 5G context, the attacker's rogue network function can deceive other network elements, redirecting traffic to achieve malicious objectives.

2.5. Potential impact and exploitation scenarios

The discovery of a critical vulnerability in the 5G network can have severe implications for the security, integrity, and availability of the network. The potential impacts include:

Confidentiality: An attacker in a Man-in-the-Middle (MiTM) position can intercept and read sensitive information traversing the network. For instance, this could include authentication credentials, or sensitive information exchanged between network functions etc. Such breaches can lead to significant privacy violations and potentially expose sensitive corporate or personal information to unauthorized parties.

Integrity: By manipulating network configuration or altering data packets, an attacker can compromise the integrity of the information being transmitted. For example, they could modify transaction details in billing services or alter control signals in critical infrastructure. This can lead to incorrect data being processed, resulting in erroneous actions and decisions based on tampered information.

Availability: The attacker can perform actions that disrupt the availability of network services. This includes dropping packets to cause Denial of Service (DoS) attacks or registering rogue network functions to misroute traffic. Such disruptions can render network services unavailable to users, causing significant operational downtimes and service interruptions.

2.6. Likelihood of Occurrence

Although 5G introduces several security advancements, its actual deployment status presents exploitable vulnerabilities. Let's explore how these scenarios might unfold:

1. **Firewall Protection:**
   Even if the vulnerable asset is behind a firewall, it is not fully protected. Firewalls are primarily designed to block unauthorized access from outside the network. However, if an attacker gains internal access—possibly through compromised partners or external connections—they can exploit vulnerabilities within the network.

2. **Security Edge Protection Proxy (SEPP):**
   SEPPs are intended to protect the roaming frontier by ensuring secure communication between roaming partners. However, as of 2024, SEPPs are not widely deployed because they are designed for standalone 5G networks, which are still relatively few. This leaves roaming communications potentially exposed to cyber threats.

3. **Service-Based Architecture (SBA) and TLS Encryption:**
   SBA in 5G networks should use TLS encryption to secure internal communications. However, TLS is not yet widely deployed. Consequently, the core network operates on clear-text HTTP-based protocols without proper protection. This lack of encryption and authentication makes it easier for attackers to intercept, alter, and manipulate data within the network.

4. **Distributed Infrastructure:**
   The distributed nature of 5G infrastructure, consisting of multiple data centers hosting various applications, increases the attack surface. This complexity introduces numerous entry points that attackers can exploit, particularly if any part of the infrastructure lacks robust security measures.

5. **External Connections and Partners**:
   The assumption that external connections and partners cannot be compromised is a significant risk. Often, these external entities act as the weakest link, providing attackers with potential entry points into the network. Once inside, attackers can leverage the lack of internal encryption and authentication to execute their attacks.

   Given these scenarios, the current state of 5G security is not only inadequate but may also be more vulnerable to cybersecurity threats than 4G. This highlights the urgent need for comprehensive security measures to protect against these critical vulnerabilities.

2.7. Tactics, Techniques, and Procedures (TTPs)

This attack method most likely relates as a new sub-technique to:

- **Network Denial of Service:** https://fight.mitre.org/techniques/FGT1498/
- **Adversary-in-the-Middle:** https://fight.mitre.org/techniques/FGT1557.504/

2.8. Steps to protect against such exploitation

Internal communication via Service-Based Architecture (SBA) should use TLS encryption. This functionality for Standalone 5G networks was introduced in later 3GPP Release 15 in 2018, when proper authentication and encryption were specified. Although the blueprint for mitigation has been available for years, implementation and deployment are different challenges. The gap between the paper release and software deployment has been significant.

Recognize the Implementation Gap:

Despite the availability of TLS encryption in 3GPP Release 15, many production networks in 2023 and 2024 were found to be operating on earlier versions that do not support TLS. This discrepancy highlights the need for focused efforts on upgrading and implementing security measures as per the latest specifications.

The primary solution is to implement proper authentication and encryption of control plane traffic between 5G core elements, as suggested by the 3GPP specifications. This ensures that all communications are secure and protected from unauthorized access.

Mitigation Alternatives:

In cases where immediate implementation of TLS is not feasible, the following mitigation steps can help minimize the risk of exploitation and negative consequences:

1. **Control Exposure of the 5G Core Network:**
   Be extra cautious about the exposure of the 5G core network and all network functions to external networks and segments. This includes connections to the Evolved Packet Core (EPC), other segments of the same mobile network, roaming partners, or the Network Exposure Function (NEF) for providing APIs for network management. All interfaces must be properly controlled, as this is the primary available frontier today.

2. **Deploy Proper Monitoring:**
   Implement robust monitoring of network communications within the 5G core. Legitimate communication between authorized nodes should be the norm, and all anomalies should be thoroughly investigated. The flexibility of launching and halting new services in 5G may allow attackers to hide their behavior in a dynamically changing infrastructure. Consider rolling out the latest available releases that support TLS communication between network functions. This is the only long-term, valid solution to ensure secure communications within the 5G core network.

03. Conclusion

Security flaws in telecom technologies have been on the agenda for several years. It is clear that proper protection is required, although this is not always available by default, especially true for older generations of cellular networks.

The 5G standards introduced several security advancements designed to guarantee a higher level of protection by design. These include the strongest encryption on the radio, a roaming frontier protected by Security Edge Protection Proxy (SEPP), and internal communication via Service-Based Architecture using TLS encryption etc.

As of 2024, only the first point—decent radio encryption—holds true. SEPPs are not widely deployed as they only work for roaming between standalone 5G networks, which remain scarce. Furthermore, TLS encryption is not widely implemented. Why?

The reasons may include additional costs or the unavailability of features, as most standalone 5G networks currently operate on 3GPP Release 15, which lacks robust authentication and encryption mechanisms.

This results in 5G being potentially more exposed to cybersecurity threats than LTE. The 5G infrastructure, comprising a distributed network of data centers hosting multiple applications, operates on clear text HTTP-based protocols without proper authentication.

Imagine a similar scenario in an enterprise network: a critical vulnerability in a Windows domain controller or a fully functional exploit for an Oracle database would be addressed immediately, even though these assets are internal and not directly exposed to the internet. This urgency stems from the understanding that hackers can breach adjacent networks to reach these critical assets. For some reason, this logic has yet to be universally applied to mobile networks.

We believe this must change. The cybersecurity community and industry stakeholders must prioritize the security of the entire 5G ecosystem to safeguard not only the infrastructure but also the organizations and people using it.

04. Additional materials

4.1. References

1. **ENISA Threat Landscape 2023**
   https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

2. **GSMA Mobile Telecommunications Security Landscape 2024**
   https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/gsma-mobile-telecommunications-security-landscape-2024/

3. **ENISA 5G Security Controls Matrix**
   https://www.enisa.europa.eu/publications/5g-security-controls-matrix

4. **MITRE 5G Hierarchy of Threats (FiGHT)**
   https://fight.mitre.org/